Norton Internet Security 2005 AntiSpyware Edition

Version 8.5

User's Guide

Norton Internet Security™ 2005 version 8.5 AntiSpyware Edition User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 8.2

Copyright Notice

Copyright © 2005 Symantec Corporation. All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, LiveUpdate, Norton AntiSpam, Norton AntiVirus, Norton Internet Security, and Norton Personal Firewall are U.S. registered trademarks of Symantec Corporation.

Microsoft, MS-DOS, MSN, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. AOL and CompuServe are registered trademarks of America Online, Inc. Pentium is a registered trademark of Intel Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Contents

Chapter 1 Installation

System requirements 5
Before installation 11
Install Norton Internet Security 12
After installation 15
For more information 17

Chapter 2 Feature summary

Security protection features 22
Virus and threat protection features 23
Spyware and other security risk protection features 25
Spam filtering features 26
Ad blocking features 28

Chapter 3 Getting started

Start Norton Internet Security 30
Start Norton Internet Security from the Internet Explorer toolbar 30
About the main window 31
Activate your product 33
Turn off security protection temporarily 35
Turn off Auto-Protect temporarily 37
Turn off spam filtering 39

Chapter 4 Responding to emergencies

What to do if a virus is found 42
If Norton AntiVirus cannot repair a file 43
Look up viruses on the Symantec Web site 44

If your product won't install 45
If your computer won't start 46
Create Emergency Disks 47
If you need to use Emergency Disks 48

Chapter 5 Frequently asked questions

Explore the Symantec service and support Web site 49
How can I find the version number? 49
If you need to uninstall 50
Troubleshoot virus and threat protection 51
Troubleshoot security protection 55
Troubleshoot Norton AntiSpam 62
Troubleshoot Ad Blocking 65
Troubleshoot LiveUpdate 66

Service and support solutions

Index

Installation

Before you install Norton Internet Security, take a moment to review the system requirements.

If you have difficulties installing Norton Internet Security, see “If your product won’t install” on page 45.

System requirements

To use Norton Internet Security, your computer must have one of the following Windows operating systems installed:

- Windows 2000 Professional
- Windows XP Professional/Home Edition
- Windows XP Tablet PC Edition
- Windows XP Media Center Edition

Installation of Norton Internet Security is not supported on Windows 95/NT 4.x, Macintosh, Linux, server versions of Windows 2000/2003/XP computers, or Windows XP 64-bit edition.

Your computer must also meet the following minimum requirements.

Operating System	Requirements
Windows 2000 Professional	■ 133-MHz or higher processor ■ 128 MB of RAM ■ 300 MB of available hard disk space ■ Internet Explorer 5.5 ■ CD-ROM or DVD-ROM drive
Windows XP Home/ Professional/ Tablet PC/Media Center Editions	■ 300-MHz or higher processor ■ 128 MB of RAM ■ 300 MB of available hard disk space ■ Internet Explorer 5.5 ■ CD-ROM or DVD-ROM drive

If you are installing on Windows 2000/XP, you must install with administrator privileges.

Supported email and instant messenger programs

Norton Internet Security adds security features to the following email and instant messenger programs.

Feature	Supported programs
Norton AntiSpam integration	Most POP3 email programs, including: ■ Microsoft® Outlook® Express 5.5 and later ■ Microsoft Outlook 2000/XP/2003 ■ Eudora® 5.0 and later ■ Netscape® Messenger 4.x ■ Netscape Mail 6.0/P ■ Yahoo! Mail and Yahoo! Mail Plus on the Web Not compatible with the following email clients and protocols: ■ AOL ■ Lotus Notes ■ IMAP ■ POP3 clients that use SSL (Secure Sockets Layer)

Feature	Supported programs
Email scanning	Most POP3 and SMTP email programs, including: ■ Microsoft Outlook Express 4, 5, 6 ■ Microsoft Outlook 97/98/2000/XP/2003 ■ Netscape Messenger 4 ■ Netscape Mail 4, 6, 7 ■ Eudora Light 3, Eudora Pro 4, Eudora 5, Eudora 6.0, Eudora 6.0J ■ Pegasus 3 ■ IncrediMail XE ■ Becky! Internet Mail 1.x, 2.0 ■ AL-Mail32 1.11 ■ Datula 1.x ■ PostPet 2.1, 2.06, 3.0 Norton Internet Security does not support the following email clients and protocols: ■ AOL ■ IMAP ■ POP3s with Secure Sockets Layer (SSL) ■ Web-based email such as Hotmail and Yahoo! Mail ■ Lotus Notes
Norton AntiVirus instant messaging scanning	■ AOL Instant Messenger 4.7 or later ■ Yahoo! Messenger 5.0 or later ■ Windows Messenger 4.7 or later ■ MSN Messenger 4.6, 4.7, 6.0 or later Version 5.0 is not supported.
Privacy Control instant messaging scanning	■ AOL Instant Messenger, version 4.3 or later ■ MSN Messenger and Windows Messenger, version 4.6 or later

About encrypted email connections

Norton Internet Security does not support email connections that use Secure Sockets Layer. Secure Sockets Layer (SSL) is a Netscape protocol designed to provide secure communications on the Internet. If you use an SSL connection to access your email, you are not protected by Norton Internet Security.

To send email messages through SSL connections, turn off Privacy Control and Norton AntiSpam.

In Norton AntiVirus, you must turn off incoming and outgoing email protection.

To send email through SSL

1. In the main window, click **Privacy Control**.
2. In the lower-right corner of the window, click **Turn Off**.
3. In the main window, double-click **Norton AntiSpam**.
4. In the lower-right corner of the window, click **Turn Off**.
5. In the main window, click **Options > Norton AntiVirus**.

   If you set a password for Options, Norton Internet Security prompts you for the password before you can continue.
6. In the Options window, click **Email**.
7. Uncheck **Scan incoming Email (recommended)**.
8. Uncheck **Scan outgoing Email (recommended)**.
9. Click **OK**.
10. Resend your email.

Compatibility with other software and hardware

Norton Internet Security works well with Symantec pcAnywhere, most routers, Internet connection sharing programs, and popular VPNs.

Symantec pcAnywhere

You should have no problems using Symantec pcAnywhere as either a client or a host with Norton Internet Security. For maximum protection on computers that run the Symantec pcAnywhere host, ensure that Norton Internet Security includes a Personal Firewall rule that limits Symantec pcAnywhere access to only the computers that should communicate with the host. Symantec pcAnywhere passwords are also necessary for maximum security.

Routers

Norton Internet Security adds to the protection provided by the router. In some cases, you might want to reduce the protection provided by the router so that you can use programs like NetMeeting or MSN Messenger. Norton Internet Security also provides features that might not be available with cable and DSL routers, such as privacy protection.

Internet connection sharing programs

For basic protection, install Norton Internet Security on the gateway computer. For maximum protection against Trojan horses or other problem programs that initiate outbound communications, install Norton Internet Security on all computers that share the connection. You must have a license for each copy of Norton Internet Security that you install.

Virtual Private Networks

Norton Internet Security works with the following Virtual Private Networks (VPNs):

- Symantec Enterprise VPN
- Symantec Gateway Security
- Nortel
- VPNremote
- PGP
- SecureRemote

With most VPNs, when the VPN client is active, you cannot see the Internet or other computers on your local network. You can see only what is available through the VPN server to which you are connected.

Before installation

See "Create Emergency Disks" on page 47.

Before you install Norton Internet Security, prepare your computer. If your computer cannot start from a CD, create Emergency Disks.

Prepare your computer

Quit all other Windows programs before you install Norton Internet Security. Other active programs may interfere with the installation and reduce your protection.

If you have a recent version of Norton Internet Security Professional, Norton Internet Security, or Norton Personal Firewall, the installer can import and use your antispam training settings. If you have an older version of these products, the installer prompts you to remove the older version.

You must also uninstall any antivirus programs that are installed on your computer. For more information, see the user documentation that came with the programs.

If you're using Windows XP

Windows XP includes a firewall that can interfere with Norton Internet Security protection features. You must turn off the Windows XP firewall you install Norton Internet Security.

To turn off the Windows XP firewall

1 On the Windows XP taskbar, click **Start > Control Panel**.

2 In the Control Panel window, do one of the following:
   - In the default Category View, click **Network and Internet Connections**, and then click **Network Connections**.
   - In the Classic View, double-click **Network Connections**.
3 Right-click the active connection icon, and then click **Properties**.
4 In the Properties window, on the Advanced tab, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
5 Click **OK**.

Install Norton Internet Security

You can install Norton Internet Security from a CD or from a file that you download. If you have not already done so, close all other Windows programs.

To install Norton Internet Security

1 Do one of the following:
   - If you are installing from a CD, insert the CD into the CD-ROM drive, and then, when the opening screen appears, click **Install Norton Internet Security**.
   - If you downloaded your copy of Norton Internet Security, double-click the file that you downloaded, and then click **Install**.

See "If the opening screen does not appear" on page 14.

2 In the Norton Internet Security Setup window, click **Next**.
3 If prompted, read the License Agreement, and then click **I accept the License Agreement**.
   If you decline, you cannot continue the installation.
4 If product key text boxes are present, type the product key for activation.
5 Click **Next**.

6 In the Pre-Install Scanner window, click **Start Scan** to scan your computer for viruses before the installation. If an infection is detected in an active program, Norton AntiVirus may close it. Save all your data before you begin.

7 Do one of the following:
- If you want to end the scan, click **Stop Scan**.
- If a virus is detected, for each file that you want to delete, click **Delete**.

8 If you want to see the results of the scan, click **View Details**, and then click **OK** to exit.

9 Click **Next**.

10 Select an installation type. Your options are:

Install Now	Install using the most common settings. This is the best choice for most users.
Custom	View an additional window that will allow you to install without accounts and Parental Control. If you do not install these features, you will have to use Add/Remove Programs in the Windows Control Panel to create accounts or use Parental Control. See "Customize your installation" on page 14.

11 Click **Browse** to select a folder into which you want to install Norton Internet Security, if it is other than the default location.

12 Click **Next**.

13 Confirm the installation location, and then click **Next** to install Norton Internet Security.

14 Do one of the following:
- To restart your computer now, click **Restart Windows Now**.
- To restart your computer later, click **Restart Windows Later**.

Your computer is not protected until you restart.

15 Click **Finish**.

Customize your installation

During installation, if you select the Custom installation type, you can select the component programs that you want to install.

To customize your installation

1 Follow the Norton Internet Security installation procedure to step 10, select **Custom**, and then click **Next**.

2 In the Install Accounts and Parental Control window, select whether you want to install Accounts and Parental Control.

If you do not install these features, you will have to use Add/Remove Programs in the Windows Control Panel to create accounts or use Parental Control.

3 Click **Next** to continue installation at step 13.

If the opening screen does not appear

Sometimes a computer's CD-ROM drive does not automatically run a CD.

To start the installation from the Norton Internet Security CD

1 On your desktop, double-click **My Computer**.

2 In the My Computer window, double-click the icon for your CD-ROM drive.

3 In the list of files, double-click **Cdstart.exe**.

After installation

After Norton Internet Security is installed and you have restarted your computer, the Configuration Wizard appears.

Use the Configuration Wizard

The Configuration Wizard lets you activate and register Norton Internet Security and complete post-installation tasks. You must be online to activate your product.

If you choose not to register the software by using the Configuration Wizard, or if registration fails for some reason, you can register by visiting the Symantec Web site at: www.symantec.com

To use the Configuration Wizard

1. In the opening Configuration Wizard window, click **Next**.
   If you downloaded your copy of Norton Internet Security, the License Agreement window appears.
2. Read the License Agreement, click **I accept the License Agreement**, and then click **Next**.
   If you decline, you cannot continue the installation.
3. In the Product Activation window, click **Activate and register your product now**.
4. Click **Next**.
5. In the first Registration window, in the drop-down list, select the Country/Region from which you are registering.
6. If you would like information from Symantec about Norton Internet Security, check the methods by which you want to receive that information, type your email address and/or your phone number, and then click **Next**.
7. If you would like to receive postal mail from Symantec, check the check box, and then type your name and address.
8. Click **Next**.

9 In the Activation window, if product key text boxes are present, type the product key for activation.

10 Verify that you are connected to the Internet, and then click **Next**.

11 In the Activation Complete window, click **Print key** to print a copy of the product key for your records, and then click **Next**.

12 In the Subscription window, review the subscription information, and then click **Next**.

13 The Next Steps window lists the following post-installation tasks that Norton Internet Security automatically performs:

Run the Home Network Wizard	Allows your computer to communicate with other computers on your network, if one exists
Run LiveUpdate	Ensures that you have the latest virus protection

If the Turn off Windows Firewall check box and the To prevent duplicate security alerts check box appear, Symantec recommends that you leave them checked and use Norton Internet Security to protect your computer.

14 Click **Finish** to begin these tasks.

For more information

The product documentation provides assistance for using Norton Internet Security. You can find the information that you need on your computer and on the Web.

Use online Help

Help is available throughout your Symantec product. Help buttons and links to more information provide assistance that is specific to the task that you are completing. The Help menu provides a comprehensive guide to all of the product features and tasks that you can complete.

To use online Help

1. At the top of the main window, click **Help & Support** > **Norton Internet Security Help**.
2. In the Help window, in the left pane, select a tab. Your options are:

Contents	Displays the Help by topic
Index	Lists Help topics in alphabetical order by key word
Search	Opens a search box in which you can type a word or phrase

You can also print any topic in Help.

To print a topic in Help

1. In the Help window, click the **Contents** tab.
2. In the Contents list, select the topic that you want to print, and then click **Print**.
3. Select whether you want to print only the selected topic or the topic and all of the subtopics under it.
4. Click **OK**.

Window and dialog box Help

Window and dialog box Help provides information about the program. This type of Help is context-sensitive, meaning that it provides help for the dialog box or window that you are currently using.

To access window or dialog box Help

❖ Do one of the following:
- In the window, click any Help link.
- In the dialog box, select **Help** or **More Info**.

Access the User's Guide PDF

The *Norton Internet Security User's Guide* is provided on the CD in PDF format. You must have Adobe Reader installed on your computer to read the PDF.

If you purchased this product as an electronic download, Adobe Reader was not included. You must download it from the Adobe Web site.

To install Adobe Reader from the CD

1. Insert the CD into the CD-ROM drive.
2. Click **Browse**.
3. In the CD window, double-click the **Manual** folder.
4. If applicable, double-click the **Adobe** folder.
5. Double-click the program file.
6. Follow the on-screen instructions to select a folder for Adobe Reader and complete the installation.

Once you have installed Adobe Reader, you can read the PDF from the CD.

To read the User's Guide PDF from the CD

1. Insert the CD into the CD-ROM drive.
2. Click **Browse**.
3. Double-click the **Manual** folder.
4. Double-click the PDF.

You can also copy a User's Guide to your hard disk and read it from there.

To read a User's Guide from your hard disk

1 Open the location into which you copied the PDF.
2 Double-click the PDF.

Symantec products on the Web

The Symantec Web site provides extensive information about all Symantec products. There are several ways to access the Symantec Web site.

To access the Web site from the Help menu

❖ Select the solution that you want. Your options are:

Help and Support	Takes you to the product support page of the Symantec Web site, from which you can access the knowledge bases and downloads for your product.
Symantec Security Response	Takes you to the Security Response page of the Symantec Web site, from which you can update your protection and read the latest information about antithreat technology.
More Symantec solutions	Takes you to the Symantec Store Web site, from which you can get product information on every Symantec product.

Within your Symantec product, the Reports page contains a link to the Symantec online Virus Encyclopedia, as does the Windows Explorer toolbar.

To access the Web site from the Reports page

1 In the main window, under Norton AntiVirus, click **Reports**.
2 On the Reports page, click **View Online Virus Encyclopedia**.

To access the Symantec Web site from Windows Explorer

1. Open Windows Explorer.
2. On the toolbar, on the Norton AntiVirus menu, click **View Virus Encyclopedia**.
   This option connects you to the Symantec Security Response Web page, from which you can search for information on all types of viruses.

To access the Symantec Web site in your browser

- On the Internet, go to www.symantec.com

Feature summary

2

Use the information in this section to familiarize yourself with the product.

This section includes the following information:

- A list of all of the features in the product
- A brief description of each feature

The feature summary can help you determine which feature to use to solve a problem. Read the feature descriptions to locate the correct component to use.

See "Use online Help" on page 17.

For more information on any of the features listed, see the online Help.

Security protection features

Norton Internet Security includes a suite of security tools that help keep your computer safe from security threats and privacy intrusions.

Security protection features include:

Personal Firewall	Protects your computer from Internet attacks, dangerous Web content, port scans, and other suspicious behavior.
Intrusion Detection	Scans each piece of information that enters and exits your computer and automatically blocks any Internet attacks.
Outbreak Alert	Notifies you of security threats affecting Internet users worldwide and recommends actions to ensure that you are protected.
Network Detector	Lets you customize security settings for different networks. This makes it easy for mobile users who connect to the Internet from the road to stay protected at all times.
Internet Explorer toolbar	Lets you customize security settings for individual Web sites without leaving your browser.
Privacy Control	Gives you several levels of control over the kind of information that users can send via the Web, email, and instant messenger programs.
Alert Assistant	Helps you understand security issues, suggests how you can resolve problems, and advises you on avoiding future security problems.
Parental Control	Lets parents choose the Web sites and newsgroups that their children can visit and the types of Internet programs that children can use.
Password protection	Protects Norton Internet Security options from unauthorized changes.

Virus and threat protection features

Norton AntiVirus provides comprehensive virus prevention, threat detection, and repair software for your computer. It automatically detects and repairs known viruses. Norton AntiVirus detects viruses and other potential risks in instant messenger attachments as well as in email messages, Internet downloads, and other files. Easy updating of the virus definitions over the Internet keeps Norton AntiVirus prepared for the latest threats. Norton AntiVirus also scans files inside of compressed files.

Norton AntiVirus continually monitors your computer and protects it from known and unknown threats using the following features:

Auto-Protect	▪ Loads into memory when Windows starts, providing constant protection while you work. ▪ Checks for viruses, spyware, and other security risks every time that you use software programs on your computer, insert floppy disks or other removable media, access the Internet, or use document files that you receive or create. ▪ Monitors your computer for any unusual symptoms that may indicate an active threat.
Automatic LiveUpdate	Updates your program and virus definitions automatically.
Compressed file protection	Detects viruses, spyware, and other security risks inside of compressed files.
Email protection	Protects incoming and outgoing email messages, preventing your computer and other computers from infection.
Instant messenger protection	Scans for and detects viruses in instant messenger attachments.

Bloodhound technology	Detects new and unknown viruses by analyzing an executable file's structure, behavior, and other attributes such as programming logic, computer instructions, and any data that is contained in the file.
Password protection	Protects Norton AntiVirus options from unauthorized changes.
Norton QuickScan	Automatically runs once LiveUpdate updates your computer with program updates and virus definitions. Checks for infections that have processes running in memory and infections that are referenced by start-up folders and files.

Spyware and other security risk protection features

Programs that are classified as security risks, including spyware and adware, can compromise your personal information and privacy. Some of the programs perform dangerous activities, including logging keystrokes and exporting sensitive data such as bank account numbers, credit card details, and passwords without your consent. They may change security settings, attempt to disable antivirus or security software, or install additional programs without permission. Other programs may perform less harmful activities such as keeping track of Web sites you visited in order to deliver customized advertising content.

Spyware and other security risk protection features include:

Security risk scan	By default, manual and scheduled scans search for spyware, adware, and other security risks. On Windows XP and Windows 2000, Auto-Protect scans for these items as well.
Security risk restore	If a scan removes a security risk program that another program relies on for functionality, you can restore the security risk program using Quarantine.
Security risk assessment	If you are unsure how to handle a program classified as a security risk, you can view the security risk assessment, which describes the level of impact a security risk program has on your computer. You can access the security risk assessment from the Detail View, which is available when scan results require input before resolving a security risk program.

Spam filtering features

As email becomes more popular, many users are receiving an increasing amount of the unsolicited commercial email messages known as spam. Not only does spam make it difficult to identify valid email messages, some spam contains offensive messages and images.

Norton AntiSpam incorporates several powerful features to reduce your exposure to unwanted online content.

Integration with email programs	Adds buttons to the toolbar in supported email programs, if you choose
Allowed and Blocked lists	■ Uses user-defined address list to expedite scanning of email ■ Accepts all mail from Allowed list ■ Treats all mail from Blocked list as spam ■ Allows and blocks email from entire domains as well as individual email addresses
Automatic import of addresses	Automatically imports lists of addresses from supported email programs to keep your list of allowed email senders in sync, if you choose
Self-training	■ Uses outgoing mail to refine spam definition ■ Adds the recipients of your email to the Allowed list, if you choose ■ Prevents spammers from using your personal email addresses to get around the spam filter
Custom spam rules	Lets you identify email addresses and text that should and should not be filtered
Yahoo! Mail and Yahoo! Mail Plus filtering	Moves spam email to a separate folder in your Yahoo! email account

Language filtering	Blocks all email written in the language or languages you specify
Automated update of spam definitions	Updates copies of Symantec spam definition files automatically (subscription required)

Ad blocking features

Many Web sites are using more aggressive techniques to draw attention to the ads on their pages. Some have begun using larger, more prominent ads, while others rely on ad windows that appear when you enter or leave the site. Along with increasing the amount of time that it takes to display Web pages, some ads contain offensive content, cause software conflicts, or use HTML tricks to open additional browser windows.

The following features can help you better control these unwanted advertisements.

Ad blocking	Blocks ads based on user-defined criteria
Pop-up blocking	Blocks pop-up windows based on user-defined criteria

Getting started

3

This section contains information about starting your Symantec product and the features that are available in the main window.

It is not usually necessary to open your Symantec product to benefit from the protection features that it provides. Automatic features that are set during installation provide you with basic protection.

Open your Symantec product to view status information, customize option settings, perform basic tasks, and temporarily disable automatic features.

Start Norton Internet Security

Norton Internet Security protects any computer on which it is installed. You do not have to start the program to be protected.

To start Norton Internet Security

❖ Do one of the following:

- On the Windows taskbar, click **Start > Programs > Norton Internet Security > Norton Internet Security**.
- On the Windows XP taskbar, click **Start > All Programs > Norton Internet Security > Norton Internet Security**.
- On the Windows desktop, double-click the **Norton Internet Security** icon.
- In the Windows System tray, double-click the **Norton Internet Security** icon.
  In Windows XP, the system tray is called the notification area.

Start Norton Internet Security from the Internet Explorer toolbar

Norton Internet Security adds a button to the Internet Explorer toolbar.

To start Norton Internet Security from the Internet Explorer toolbar

❖ On the Internet Explorer toolbar, click the Norton Internet Security icon, and then click **Configure security settings**.

You may not be able to access the Norton Internet Security icon on the Internet Explorer toolbar, depending on your computer's configuration.

To display the Norton Internet Security button

❖ In Internet Explorer, on the View menu, click **Toolbars > Norton Internet Security**.

About the main window

Use the main window to access program components, set options, and access online Help.

To explore the main window

1. On the left side of the main window, select a category, such as Statistics or Subscription Status.
   A description or an expanded list of options appears in the center of the window.
2. At the top of the main window, click a button. Your options are:

Block Traffic/Allow Traffic	Stops and starts all communication to and from your computer.
LiveUpdate	Starts LiveUpdate, where you can update threat definitions, Norton Internet Security, and any other installed Symantec products.
Options	Customizes general features of Norton Internet Security.
Help & Support	Accesses Help for Norton Internet Security.

3 Inside the main window, under System Status, click any of the feature names to see a brief description of the feature and access configuration options for the feature.

Activate your product

Product activation reduces software piracy and ensures that you have received genuine Symantec software.

If you did not activate your product when first prompted, you will receive an Activation Needed alert every day until you activate the product.

You must activate your product within the time period specified by the alert or the product will stop working.

You can activate your product from the Activation Needed alert or from the Activation option on the Help menu. Activation should take just a few minutes.

To activate your product from the Activation Needed alert

1. In the alert, click **Activate Now**.
2. Click **OK**.
3. On the Activation screen, click **Next**.
4. On the Activation Successful screen, click **Finish**.

To activate your product from the Help menu

1. At the top of the main window, click **Help and Support** > **Activation**.
2. On the Activation screen, click **Next**.
3. On the Activation Successful screen, click **Finish**.

If you have problems activating

If you cannot connect to the Symantec servers to activate your product, first check to see if you have parental control software or an ISP that might be blocking the connection. If that doesn't resolve the issue, you can activate by phone.

Check for connectivity blocking

A connectivity problem can occur if you are using parental control software or are using an ISP that provides parental controls. If you suspect that parental controls are blocking the connection, configure the parental controls so that they do not block the activation procedure. You will need to log in to your parental control software as an administrator, or log in to the Internet through your ISP as an administrator, to change your configuration.

Activate by phone

If parental controls are not the problem, or if you cannot reconfigure your parental controls to resolve the issue, you can activate by phone.

To activate by phone

1. Disconnect from the Internet.
2. Attempt activation again.
3. After the connection fails (which could take a minute or two), select **Activate my software by phone**, then click **Next**.
4. Follow the prompts provided.

Turn off security protection temporarily

There may be times when you want to temporarily turn off security protection. For example, you might want to see if it is preventing a Web page from appearing as expected.

Only Supervisor users can temporarily turn off security protection. Child and Teenager users cannot turn off any portion of the program.

Turning off security protection also turns off all of the individual security features.

To turn off security protection temporarily

1. In the main window, click **Security**.
2. In the lower-right corner of the window, click **Turn Off**.
3. In the pop-up window that appears, in the drop-down list, select how long you want to turn off security protection, and then click **OK**.

To ensure that your computer remains protected, you can turn on security protection manually if you complete your task before the time that you specified concludes.

To turn on security protection

1. In the main window, click **Security**.
2. In the lower-right corner of the window, click **Turn On**.

If the Norton Internet Security icon appears in the Windows system tray, you can use it to turn on and turn off security protection.

To turn off security protection using the icon in the Windows system tray

1. In the Windows system tray, right-click the Norton Internet Security icon, and then click **Disable Norton Internet Security**.
2. In the pop-up window that appears, in the drop-down list, select how long you want to turn off security protection, and then click **OK**.

To ensure that your computer remains protected, you can turn on security protection manually if you complete your task before the time that you specified concludes.

To turn on security protection using the icon in the Windows system tray

❖ In the Windows system tray, right-click the Norton Internet Security icon, and then click **Enable Norton Internet Security**.

You can also turn off individual security features. For example, you might want to see if the Personal Firewall is preventing a program from operating as expected.

To turn off a security feature

1 In the main window, select the feature that you want to turn off.

2 In the lower-right corner of the window, click **Turn Off**.

3 In the pop-up window that appears, in the drop-down list, select how long you want to turn off the feature, and then click **OK**.

To ensure that your computer remains protected, you can turn on the feature manually if you complete your task before the specified time frame concludes.

To turn on a security feature

1 In the main window, select the feature that you want to turn on.

2 In the lower-right corner of the window, click **Turn On**.

Turn off Auto-Protect temporarily

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses, Trojan horses, worms, and other malicious threats. It checks programs for viruses as they are run and monitors your computer and removable media for any activity that might indicate the presence of a virus. When a virus or virus-like activity is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. If you will be performing such an activity and want to avoid the warning, you can turn off Auto-Protect.

If you have set a password for Options, Norton Internet Security asks you for the password before you can view or change the settings.

To turn off Auto-Protect

1. In the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Auto-Protect**.
3. In the Auto-Protect pane, uncheck **Enable Auto-Protect**.
4. In the Options popup window, select the period during which you want Auto-Protect turned off.

To turn on Auto-Protect

1. In the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Auto-Protect**.
3. In the Auto-Protect pane, check **Enable Auto-Protect**.

If the Norton Internet Security icon is visible in the Windows system tray, you can use it to turn on and turn off Auto-Protect.

To turn on or turn off Auto-Protect using the icon in the Windows system tray

❖ In the Windows system tray, right-click the Norton Internet Security icon, and then do one of the following:

- Check **Enable Auto-Protect** to turn on Auto-Protect.
- Uncheck **Enable Auto-Protect** to turn off Auto-Protect.

Turn off spam filtering

By default, Norton AntiSpam remains active once it is installed. If for any reason you want to temporarily disable it, you can turn it off from within the program itself.

To turn off spam filtering

1. In the main window, under Norton AntiSpam, click **Status & Settings**.
2. In the System Status pane, click **AntiSpam**.
3. On the right side of the main window, click **Turn Off**.

To turn on spam filtering

1. In the main window, under Norton AntiSpam, click **Status & Settings**.
2. In the System Status pane, click **AntiSpam**.
3. On the right side of the main window, click **Turn On**.

Responding to emergencies

4

If you have an emergency, read these sections to try to find the solution to your problem.

Common problems include:

- Virus threats
- Trouble restarting your computer

If you purchased this product to address any of the problems listed above, read these sections first. Immediate installation of the product may not always provide the best solution to your problem.

What to do if a virus is found

If after reviewing the information in this chapter, you have not resolved your problem, see "Frequently asked questions" on page 49.

Viruses can be found during a manual or scheduled scan or by Auto-Protect when you perform an action with an infected file. Threats and security risks can appear during an instant messenger session, when sending an email message, or during a manual or scheduled scan.

If Norton AntiVirus finds a virus or a file containing a virus or a potential security risk on your computer, there are several possible resolutions to the problem:

Resolution	Action
Repair	Removes the virus from the file, or if the threat is a worm or Trojan horse, deletes the file.
Quarantine	Makes the file inaccessible by any program other than a Symantec antivirus program. You cannot accidentally open the file and spread the virus, but you can still evaluate it for possible submission to Symantec.
Delete	Removes the virus from your computer by deleting the file that contains the virus, worm, or Trojan horse. Delete should be used only if the file cannot be repaired or quarantined.
Detail View	Lists infections or programs that Norton AntiVirus is unable to automatically remove. However, the Detail View window lets you launch the Symantec Web site for a tool or instructions to remove these risks.

See "Use online Help" on page 17.

The online Help contains more information about this feature.

If Norton AntiVirus cannot repair a file

One of the most common reasons that Norton AntiVirus cannot automatically repair an infected file is that you do not have the most up-to-date virus definitions. Before running LiveUpdate to update your virus definitions, ensure that Norton QuickScan is turned on (it is turned on by default). After LiveUpdate updates your virus definitions, Norton QuickScan automatically checks for infections that have processes running in memory or infections that are referenced by start-up files and folders.

If that does not work, read the information in the Scan Complete window to identify the types of files that cannot be repaired, and then depending on the file type, take one of the following actions:

File type	Action
Infected files with .exe, .doc, .dot, or .xls file name extensions (any file can be infected)	Use the Detail View to solve the problem. For more information, see the online Help. See "Use online Help" on page 17.
Hard disk master boot record, boot record, or system files (such as IO.SYS or MSDOS.SYS) and floppy disk boot record and system files	Replace using your operating system disks.

Look up viruses on the Symantec Web site

The Symantec Web site contains a complete list of all known viruses and related malicious code, along with descriptions. You must be connected to the Internet to look up viruses.

To look up viruses

1. On the left side of the main window, under Norton AntiVirus, click **Reports**.
2. In the Reports pane, click **View Online Virus Encyclopedia**.
   The Symantec Web site opens in your Internet browser.
3. Use the links on the Web page to access the virus information that you want to view.

If your product won't install

You must be running Windows in order to install your Symantec product.

If you try to install your product on a computer that has a virus and you choose not to run the Symantec Pre-Install Scanner, start over and run the Symantec Pre-Install Scanner as directed.

If you cannot run the Norton AntiVirus Pre-Install Scanner, but you can connect to the Internet, go to http://security.symantec.com and run virus detection from the Symantec Security Check Web site.

Once the virus has been repaired, delete the installation files that were left behind in the folder after you tried to install the first time.

To delete remaining installation files

1. On the Windows taskbar, click **Start > Run**.
2. In the Run dialog box, type **%TEMP%**
3. Click **OK**.
4. Close the window.
5. After you delete the temporary files, begin installation again and run the Symantec Pre-Install Scanner to be sure that you have removed all of the viruses.

If your computer won't start

If you have a virus or threat on your computer, you need to start the computer from an uninfected disk to remove the virus.

Suggestion	For more information
Restart from the CD and scan your computer's hard disk for viruses.	See "Scan for viruses using the CD" on page 46.
If you have access to another computer, create a set of Emergency Disks and start your computer from the Emergency Disks.	See "Create Emergency Disks" on page 47. See "If you need to use Emergency Disks" on page 48.

Scan for viruses using the CD

You might need to change your computer's BIOS Setup options to start from the CD-ROM drive. To do so, see the documentation that came with your computer.

To start from the CD and scan for viruses

1. Insert the CD into the CD-ROM drive.
2. Restart your computer.
   Your computer displays the following information:
   - 1 Boot from Hard Drive
   - 2 Boot from CD-ROM
3. Press **2 Boot from CD-ROM** to restart from the CD. After the computer restarts, the Emergency program automatically begins to scan for and remove viruses.
4. When Norton AntiVirus has finished scanning, remove the CD from your CD-ROM drive.

Create Emergency Disks

Emergency Disks are used to start your computer in case of a problem.

If your computer can start from a CD, you can use the product CD in place of Emergency Disks and do not need to create them. If you cannot start your computer from a CD, you can use the instructions below to create Emergency Disks on another computer.

If you downloaded the software, the program for creating Emergency Disks (NED.exe) is included in the download. Locate the downloaded software on your hard disk, and then follow the instructions to create emergency disks, shown below.

You can also download the program for creating Emergency Disks (NED.exe). Go to http://www.symantec.com/techsupp/ebd.html. Follow the instructions that are included in the download to create the Emergency Disks.

You will need several formatted 1.44-MB disks.

To create Emergency Disks

1. Insert the CD into the CD-ROM drive.
2. Click **Browse CD**.
3. Double-click the **Support** folder.
4. Double-click the **Edisk** folder.
5. Double-click **NED.exe**.
6. In the Welcome window, click **OK**.
7. Label the disk as instructed, and then insert it into drive A.
8. Click **Yes**.
9. Repeat steps 7 and 8 for the subsequent disks.
10. When the procedure is complete, click **OK**.
11. Remove the final disk from drive A.
12. Test the first disk in the set to ensure that you can use it to restart your computer.
13. Store the Emergency Disk set in a safe place.

If you need to use Emergency Disks

You can use Emergency Disks to restart your computer and scan for viruses or run DOS-based recovery utilities.

To use Emergency Disks

1. Insert Emergency Disk 1 into drive A, and then restart your computer.
   The Emergency program runs in DOS.
2. Select the program that you want to run.
   For DOS program help, press the **F1** key while you are running the program.
3. Follow the on-screen instructions for inserting and removing the Emergency Disks.
4. When the Emergency program is done, remove the Emergency Disk from drive A, and then restart your computer.

Frequently asked questions

5

The information in this chapter will help you solve the most frequently encountered problems.

Explore the Symantec service and support Web site

On the Symantec service and support Web site, you can find the latest protection and program updates, patches, online tutorials, Knowledge Base articles, and virus removal tools.

To explore the Symantec service and support Web site

1. On the Internet, go to www.symantec.com/techsupp
2. Follow the links to the information that you want.

How can I find the version number?

You can check the version number of your product on your computer.

To check the version number

1. Start your product.
2. Click **Help and Support**.
3. On the Help menu, click **About <your product name>**.
4. If applicable, in the About dialog box, select your product name.

If you need to uninstall

See "Use online Help" on page 17.

Instructions for uninstalling are available in the online Help.

Troubleshoot virus and threat protection

Check here for possible solutions to issues that might arise with Norton AntiVirus.

How do I make Auto-Protect load when I start my computer?

Failure to load Auto-Protect may be due to one of the following situations:

You may have started Windows in safe mode. Windows restarts in safe mode if the previous shutdown did not complete successfully. For example, you may have turned off the power without choosing Shut Down on the Windows Start menu.

To restart Windows

1. On the Windows taskbar, click **Start > Shut Down**.
2. In the Shut Down Windows dialog box, click **Restart**.
3. Click **OK**.

Norton AntiVirus may not be configured to start Auto-Protect automatically.

To set Auto-Protect to start automatically

1. In the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Auto-Protect**.
3. Ensure that **Start Auto-Protect when Windows starts up** is checked.

How do I stop a virus that continues to infect my files after I have scanned and removed the virus?

A virus may continue to infect files for several reasons.

The virus might be in a program file with an unusual extension for which Norton AntiVirus is not configured to search.

To reset Norton AntiVirus scanning options

1. In the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under System, click **Manual Scan**.
3. Under Which file types to scan for viruses, click **Comprehensive file scanning**.
4. Click **Manual Scan > Bloodhound**.
5. Ensure that Enable Bloodhound heuristics is checked, and then click **Highest level of protection**.
6. Click **OK**.
7. Scan all of the disks that you use and repair all infected files.

The source of the infection could be a floppy disk. Scan all of the floppy disks that you use to ensure that they are free of viruses.

The virus might be remaining in memory after you remove it from the boot record. It then reinfects your boot record. If the problem is a Trojan horse or worm that was transmitted over a shared network drive, you must disconnect from the network or password protect the drive to let Norton AntiVirus delete the problem.

Why is Norton AntiVirus unable to repair my infected files?

If Norton AntiVirus cannot repair your infected files, you may not have the most current virus protection on your computer. Update your virus definitions regularly to protect your computer from the latest viruses.

If, after using LiveUpdate, the virus cannot be removed, the file may be corrupted, or contain a new virus. Do one of the following:

- Quarantine the file and submit it to Symantec.
- Replace the infected file with a clean copy, if one exists, and delete the infected file.

Why am I unable to receive email messages?

If you are using a firewall, it may block access to the Internet features of Norton AntiVirus and prevent receipt of Email messages.

You can temporarily turn off email protection and attempt to download your email messages again.

To temporarily turn off incoming email protection

1. In the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under Internet, click **Email**.
3. Uncheck **Scan incoming Email**.
4. Click **OK**.
5. Download your email messages.
6. Check Scan incoming Email to turn email protection back on.

Your email client may have timed out. Make sure that timeout protection is turned on.

If you continue to experience problems downloading email messages, turn off email protection.

To turn off email protection

1. In the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under Internet, click **Email**.
3. Uncheck **Scan incoming Email**.
4. Uncheck **Scan outgoing Email**.
5. Click **OK**.

Why am I unable to send email messages?

If you get the message Norton AntiVirus was unable to send your email message because the connection to your email server was disconnected, your email client may be set to automatically disconnect after sending and receiving email messages. To resolve this issue, turn off this option within your email client. Consult your email client manual for instructions on how to do this.

If you are using a firewall, it may block access to the Internet features of Norton AntiVirus.

For Norton AntiVirus to scan outgoing email messages for viruses, it intercepts and scans the messages before they are sent to your email provider. To resolve this issue, turn off Norton AntiVirus outgoing email scanning.

To turn off outgoing email scanning

1. In the main window, click **Options**.
   If a menu appears, click **Norton AntiVirus**.
2. In the Options window, under Internet, click **Email**.
3. Uncheck **Scan outgoing Email**.
4. Click **OK**.

Troubleshoot security protection

Check here for possible solutions to issues that might arise with Norton Internet Security.

Does Norton Internet Security work with my ISP's proxy server?

Norton Internet Security works with most proxy servers. However, you might have to change some settings to maintain full protection.

To determine whether the Personal Firewall works with your proxy server

1. In the main window, click **Statistics**.
2. In the Statistics window, click **More Details**.
3. Under Network, look at the All Bytes Sent and All Bytes Received counters.
4. Use your browser to connect to a Web site.
   The All Bytes Sent and All Bytes Received counters in the Norton Internet Security Statistics window should increase as you access Web pages. This indicates that the Personal Firewall is correctly configured to work with your proxy server.
5. To close the Norton Internet Security Statistics window, on the File menu, click **Exit**.

If the All Bytes Sent and All Bytes Received counters stay at 0, then the Personal Firewall is probably not monitoring the port used by your proxy server. You need to determine which ports your proxy server is using for HTTP communications, and then configure the Personal Firewall to monitor those ports.

To determine which port to monitor for HTTP communication

1. Use your browser to connect to a Web site.
2. In the main window, click **Statistics**.
3. In the Statistics window, click **View Logs**.
4. On the Connections tab, in the Remote Service Port column, look at the information.
   There should be a port number following the IP address of the site that you viewed with your browser. This number is the port number that is used to access your proxy server for your Web connection.
5. Record the port number.

To specify which ports to monitor for HTTP communication

1. At the top of the main window, click **Options**. If a menu appears, click **Norton Internet Security**.
2. On the Firewall tab, under HTTP Port List, do one of the following:
   - To add a port to the HTTP Port List, click **Add**, and then type the number of the port that you want to monitor for HTTP communication.
   - To remove a port from the HTTP Port List, select the port number in the HTTP Port List, and then click **Remove**.
3. Click **OK**.

Can Norton Internet Security protect a Web server?

To protect a Web server, you must create a firewall rule that allows inbound TCP connections on port 80. The easiest way to create these rules is via a Norton Internet Security alert.

To create rules for a Web server using an alert

1. On the Web server, view your Web site by typing the IP address in the address bar of your browser. An alert appears.
2. In the alert, on the drop-down menu, click **Automatically configure Internet access**.
3. Click **OK**.

Can Norton Internet Security protect an FTP server?

To let an FTP server run behind Norton Internet Security, you must create the following rules:

- Allow inbound TCP connections on port 21.
- Allow outbound TCP connections on port 22.
- Allow inbound TCP connections on ports 1024 to 5000.

The easiest way to create these rules is via an alert.

To create rules for an FTP server using an alert

1. In the address bar of your browser, type **ftp://** followed by the IP address of your FTP server. An alert appears.
2. In the alert, on the drop-down menu, click **Automatically configure Internet access**.
3. Click **OK**.

What is wrong with this Web site?

If you cannot connect to a Web site with Norton Internet Security turned off, there might be a problem with the Internet or your Internet service provider. If your connection is working, it's possible a Norton Internet Security feature is preventing you from viewing the site.

Problem	Solution
It could be Cookie Blocking	Many Web sites require that cookies be enabled on your computer to display correctly.
It could be Parental Control	If you have set up Parental Control to block certain categories of Web sites, it may be blocking the site that you are attempting to view. When Parental Control blocks a site, it always displays a message telling you that the site is blocked.
It could be a firewall rule	A firewall rule might be blocking the Web site. When this happens, you will usually see a message saying that you could not connect.
It could be ActiveX or Java blocking	Some Web sites display only ActiveX controls or Java applets. If you are blocking them, nothing appears on these sites.
It could be Content Blocking	Sometimes blocking content on the Internet prevents an entire Web site from appearing in your browser.

Why can't I post information online?

If you are unable to post information to a Web site, it may be because Privacy Control is blocking the information. Check the Private Information list to see if the information that you are trying to enter is being blocked.

Why did an email message I sent never arrive?

If you choose to block an email message containing private information, Norton Internet Security immediately deletes the email message. Your email program will indicate that the message was sent, but the recipient will not receive it.

If your email program maintains copies of sent messages in its Sent or Out folder, you can reopen the email message, remove the private information, and send the message again.

Why won't a program connect to the Internet?

You might not be able to use a program to connect to the Internet for any of the following reasons.

Problem	Solution
The program might belong in a category of programs that is restricted for this account.	Determine if the program belongs in a restricted category, and then block or permit category access.
There is no firewall rule that lets the program create a connection to the Internet.	Add a firewall rule for the program.
There is a firewall rule that blocks the program from creating a connection to the Internet.	Modify the firewall rule for this program to permit it to connect to the Internet.
Norton Internet Security could be blocking your account from using this program on the Internet.	Use Parental Control to adjust account settings.

Why doesn't Norton Internet Security notify me before letting programs access the Internet?

If Automatic Program Control is turned on, Norton Internet Security creates rules for programs that it recognizes and notifies you the first time that a recognized program accesses the Internet. You will not be notified of subsequent access attempts.

Why can't I print to a shared printer or connect to a computer on my local network?

Norton Internet Security blocks the use of Microsoft networking to prevent someone from connecting to your computer over the Internet.

To allow the use of your local network, including file and printer sharing, place the computers on your local network in the Trusted Zone.

Why can't I connect to the Internet via my cable modem?

If your network accesses the Internet via a cable connection, you may need to make your computer's NetBIOS name visible. While the NetBIOS name is visible, the files and folders on your computer remain hidden.

To make your NetBIOS name visible

1. In the main window, double-click **Personal Firewall**.
2. In the Personal Firewall window, on the Advanced tab, click **General**.
3. In the General Rules dialog box, click **Default Inbound NetBIOS Name**.
4. Click **Modify**.
5. In the Modify Rule dialog box, on the Action tab, click **Permit**.
6. Click **OK**.
7. In the General Rules dialog box, click **OK**.
8. In the Personal Firewall window, click **OK**.

Some Internet service providers scan the ports on users' computers to ensure that they are keeping to their service agreements. Intrusion Detection might interpret this as a malicious port scan and stop communications with your cable system. If this occurs, you need to let your cable provider run port scans.

To allow ISP port scans

1. In the main window, double-click **Intrusion Detection**.
2. In the Intrusion Detection window, on the AutoBlock tab, click **Exclusions**.
3. In the Exclusions dialog box, select the IP address your ISP uses for port scans.
   Your ISP can provide this information.
4. Click **Exclude**.
5. Click **OK**.

How can a Web site get my browser information?

The Browser Privacy settings prevent your browser from sending browser information. However, some diagnostic sites on the Internet might report browser information even though the Browser Privacy settings are blocking it.

If you are blocking Java, ActiveX, or scripts, the site might be using one of these methods to retrieve the information. Sometimes when Web servers do not get the information from the browser, they use the last piece of browser information that they received instead. You might see the information from the last person who viewed the site.

Privacy Control filters cookies by removing them from the responses your computer sends to Web sites. Some sites display information about your browser by using JavaScripts that run within the browser and do not communicate with the Web site. Since the JavaScript runs entirely locally, the Web site does not have access to that information.

Troubleshoot Norton AntiSpam

Check here for possible solutions to issues that might arise with Norton AntiSpam.

Why do I still receive spam?

Several factors make it difficult to completely eliminate spam. For example, different people will consider different classes of email messages to be unwelcome or intrusive. Some, for instance, do not want to receive anything they have not specifically requested. Others are glad to receive items regarding their interests or profession even if they have not specifically requested them.

Also, for every new method that is developed to control spam, there are numerous spammers trying to develop ways to circumvent it. This on-going contest of wills and skills is one reason Symantec maintains up-to-date spam definitions.

Finally, not all unwanted messages are unauthorized. Some companies require you to accept email messages in exchange for certain services. Many users do not understand that in doing so they are agreeing to, in effect, accept spam.

How will email messages from addresses on my Blocked list be handled?

Norton AntiSpam moves email messages from these addresses to the Norton AntiSpam folder and marks them in the subject line as spam.

What if I mistakenly put an address on the Blocked list?

The only result will be that you will not see any email messages from this address in your main list. But if you periodically review the contents of your spam folder, you will be able to retrieve any email messages from that address and then correct the entry in your list.

Why did an email message someone sent me never arrive?

Some legitimate email messages may contain elements that are characteristic of spam messages. This may have caused Norton AntiSpam to incorrectly identify the message as spam. Depending upon the filters you have created in your email program, the message may be in your spam or trash folder.

To avoid losing email messages from this person, add them to your Allowed list.

Does Norton AntiSpam check for email-borne viruses?

Norton AntiSpam does not check for viruses. To scan incoming email messages for viruses, you must install Norton AntiVirus.

Why does so much spam include clusters of meaningless characters?

These and other unusual elements in spam are intended to confuse spam filters that look for keywords.

How do I keep my spam protection updated?

To some degree, Norton AntiSpam updates itself by learning from your outgoing email messages and other data. However, to receive up-to-date copies of Symantec spam definitions, you must subscribe to this service. You can then choose to have these definitions updated automatically.

Why do I need a subscription to spam definitions?

Though the product is self-training, local spam definitions are developed only by the criteria you input and from the sample of email messages you process. Symantec spam definitions are developed from a much larger set of information and can prevent you from seeing many of the more common types of spam.

Troubleshoot Ad Blocking

Check here for possible solutions to issues that might arise with Ad Blocking.

Does Ad Blocking block all advertising on the current page?

Ads that are integrated with standard content–for instance text statements–will not be blocked.

Will Pop-up Window Blocking block all pop-ups or only pop-up ads?

Ad Blocking blocks all pop-ups that are started automatically during a Web page load. If a site uses pop-ups for special alerts or additional information, you might want to disable Pop-up Window Blocking while viewing that site.

Are there security issues associated with advertisements?

While clicking on an ad should only display more information or direct you to another site, some advertisers will use ads to entice you into installing new functionality on your system. These may range from adding new menus to installing spyware. You should be especially wary of ads that invite you to install novelty cursors or other entertaining add-ons. These frequently include user agreements that require you to allow companies to track your browsing or to provide them with personal information, among other things. Such clauses are typically hidden deep in the text where many users will not bother to read them.

Troubleshoot LiveUpdate

Check here for possible solutions to issues that might arise with LiveUpdate.

What if I can't use LiveUpdate?

When new updates become available, Symantec posts them on the Symantec Web site. If you can't run LiveUpdate, you can obtain new updates from the Symantec Web site.

To obtain updates from the Symantec Web site

1. On the Internet, go to securityresponse.symantec.com
2. Follow the links to obtain the type of update that you need.

What if I run LiveUpdate on an internal network?

If you run LiveUpdate on a computer that is connected to a network that is behind a company firewall, your network administrator might set up an internal LiveUpdate server on the network. LiveUpdate should find this location automatically.

If you have trouble connecting to an internal LiveUpdate server, contact your network administrator.

Why is Automatic LiveUpdate having problems connecting?

Automatic LiveUpdate does not recognize proxy settings that are configured in the Internet Options Control Panel. To ensure that your proxy settings are used by Automatic LiveUpdate, you must configure them in the Symantec LiveUpdate Control Panel.

Service and support solutions

The Service & Support Web site at http://service.symantec.com supports Symantec products. Customer Service helps with nontechnical issues such as orders, upgrades, replacements, and rebates. Technical Support helps with technical issues such as installing, configuring, or troubleshooting Symantec products.

Methods of technical support and customer service can vary by region. For information on support offerings in your region, check the appropriate Web site listed in the sections that follow.

If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

Customer service

The Service & Support Web site at http://service.symantec.com tells you how to:

- Subscribe to Symantec newsletters.
- Locate resellers and consultants in your area.
- Update your product registration.
- Find out about orders, returns, or a rebate status.
- Access Customer Service FAQs.
- Post a question to a Customer Service representative.
- Obtain product information, literature, or trialware.

For upgrade orders, visit the Symantec Store at: http://www.symantecstore.com

Technical support

Symantec offers two technical support options for help with installing, configuring, or troubleshooting Symantec products:

- Online Service and Support
  Connect to the Symantec Service & Support Web site at http://service.symantec.com, select your user type, and then select your product and version. You can access hot topics, Knowledge Base articles, tutorials, contact options, and more. You can also post a question to an online Technical Support representative.
- PriorityCare telephone support
  This fee-based (in most areas) telephone support is available to all registered customers. Find the phone number for your product at the Service & Support Web site. You'll be led through the online options first, and then to the telephone contact options.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued 60 days later. Technical information may still be available through the Service & Support Web site at: http://service.symantec.com

Subscription policy

If your Symantec product includes virus, firewall, or Web content protection, you may be entitled to receive updates via LiveUpdate. Subscription length varies by Symantec product.

After your initial subscription ends, you must renew it before you can update your virus, firewall, or Web content protection. Without these updates, you will be vulnerable to attacks.

When you run LiveUpdate near the end of your subscription period, you are prompted to subscribe for a nominal charge. Simply follow the instructions on the screen.

Worldwide service and support

Technical support and customer service solutions vary by country. For Symantec and International Partner locations outside of the United States, contact one of the service and support offices listed below, or connect to http://service.symantec.com and select your region or language under Global Support.

Service and support offices

North America

Symantec Corporation
555 International Way
Springfield, OR 97477
U.S.A.

http://www.symantec.com/

Australia and New Zealand

Symantec Australia
Level 2, 1 Julius Avenue
North Ryde, NSW 2113
Sydney
Australia

http://www.symantec.com/region/reg_ap/
+61 (2) 8879-1000
Fax: +61 (2) 8879-1001

Europe, Middle East, and Africa

Symantec Ltd
Consumer Services & Support
PO Box 5689
Blanchardstown, Dublin 15
Ireland

http://www.symantec.com/region/reg_eu/
+353 (1) 811 8032

Latin America

Symantec Brasil
Market Place Tower
Av. Dr. Chucri Zaidan, 920
12º andar
São Paulo – SP
CEP: 04583-904
Brasil, SA

Portuguese:
http://www.service.symantec.com/br
Spanish:
http://www.service.symantec.com/mx
Brazil: +55 (11) 5189-6300
Mexico: +52 55 5322 3681 (Mexico DF)
01 800 711 8443 (Interior)

August 12, 2004

Index

A

activate
  and register 15
  software 15
activation
  activation problems 33
  phone 34
  procedure 33
active content, troubleshooting 58
ActiveX controls 58
Ad Blocking, troubleshooting 65
Adobe Reader
  installing 18
  using to view PDF 18
adware
  protection features 25
  See also security risks
Alert Assistant 22
Automatic LiveUpdate and proxy settings 66
Auto-Protect
  description 37
  failure to load 51
  failure to load on startup 51
  functions 23
  turn off 37
  turn on 37

B

blocking
  browser information 61
blocking *(continued)*
  cookies 58
Bloodhound technology, description 24
booting, Auto-Protect failure to load 51
browser information 61

C

CD-ROM, drive, starting from 46
checking for version number 49
computer, emergency procedures 41
computer requirements 5
Configuration Wizard
  features 15
  using 15
Cookie Blocking, troubleshooting 58
cookies 58
creating, Emergency Disks 47
customizing installation 14

D

description of product features 21
disabling
  security protection 35
  Windows XP firewall 11
displaying the Internet Explorer toolbar 30
downloading protection from Symantec Web site 66

drive A, using for Emergency Disks 47

E

email protection 23
emergency, recovery procedures 41
Emergency Disks
  creating 47
  using 48

F

features
  about 22
  ad blocking 28
  automatic update 27
  Configuration Wizard 15
  email filtering 26
  main window 31
  security protection 22
  security risk protection 25
  virus and threat protection 23
file extensions
  about 43
  unusual 51
files, reinfected after virus removal 51
firewall
  and LiveUpdate 66
  and network 66
  troubleshooting 58
  Windows XP 11
firewall rules
  for FTP servers 57
  for Web servers 57
folders and NetBIOS 60
FTP servers 57

H

Help
  online 17
  window and dialog box 18
Help & Support menu 31

I

infected files
  cannot repair 52
  reinfected 51
installing
  components 14
  Norton Internet Security 12
instant messenger
  supported programs 8
  virus protection 23
Internet
  Knowledge Base articles 49
  Symantec service and support Web site 49
  Symantec Web sites 19
Internet Explorer toolbar 22
Intrusion Detection 22

J

Java applets 58

K

keystroke logging 25

L

LiveUpdate button, main window 31

M

main window
  features 31
  LiveUpdate button 31
  Options button 31

N

NetBIOS, making name visible 60
Network Detector 22
networks
  internal LiveUpdate server 66

networks *(continued)*
troubleshooting 60
using LiveUpdate 66
Norton AntiSpam
Allowed and Blocked lists 26
spam blocking features 26
troubleshooting 62
Norton QuickScan 24

O

online, Virus Encyclopedia 44
online Help 17
operating systems 5
Options button, main window 31

P

Parental Control 22
password protection
feature 24
options 22
Personal Firewall
about 22
troubleshooting rules 58
phone activation 34
Pop-up Window Blocking
about 28
troubleshooting 65
ports, determining active HTTP 56
post-installation tasks 15
Privacy Control 22
problems
activation 33
troubleshooting Ad Blocking 65
troubleshooting LiveUpdate 66
troubleshooting Norton AntiSpam 62
troubleshooting security protection 55
troubleshooting virus and threat protection 51
proxy servers 55

R

register your software 15
removing
other antivirus programs 11
previous copies of Norton Internet Security 11
repairing, viruses 23
restarting, Windows in safe mode 51
restarting after installation 13

S

safe mode 51
scanning before installation 13
security protection, turning off 35
Security Response Web page 19
security risks
about 42
assessment 25
finding 42
protection features 25
restoring 25
scan 25
Service and Support 67
spyware
protection features 25
See also security risks
starting
Auto-Protect 23
Auto-Protect failure to load 51
Bloodhound technology 24
from the CD-ROM drive 46
spam blocking 39
virus protection 23
starting your Symantec product 29
startup, Auto-Protect failure to load 51
stopping, spam blocking 39
summary of product features 21
Symantec Security Response 19
Symantec Web sites 19, 66
look up viruses 44

system requirements 5

T

Technical Support 19, 67
threats, how Norton AntiVirus detects 23
toolbar, displaying in Internet Explorer 30
Trojan horses, transmitted over a network 52
troubleshooting
  activation 33
  ActiveX and Java 58
  Ad Blocking 65
  browser information 61
  cable modem connections 60
  Cookie Blocking 58
  firewall rules 58
  LiveUpdate 66
  networks 60
  Norton AntiSpam 62
  printing 60
  Web sites 58

U

uninstalling
  location of instructions 50
  other antivirus programs 11
  previous copies of Norton Internet Security 11
unknown viruses 24
updating
  from Symantec Web site 66
  protection 66
User's Guide PDF
  on CD 18
  opening 18

V

version number, checking 49
virtual private network (VPN) 10
Virus Encyclopedia 19
virus protection, updates 23
viruses
  automatic protection 23
  descriptions 23
  looking up on the Symantec Web site 44
  unknown 24
  viewing descriptions 44

W

Web servers 57
Web sites 19, 49, 66
Windows
  operating systems 5
  safe mode 51
  system tray icon 35, 38
Windows 2000 system requirements 6
Windows XP system requirements 6

Symantec Software License Agreement
Norton Internet Security™

IMPORTANT: PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE "ACCEPT" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE "I DO NOT ACCEPT" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL, MAKE NO FURTHER USE OF THE SOFTWARE, AND CONTACT SYMANTEC CUSTOMER SERVICE FOR INFORMATION ON HOW TO OBTAIN A REFUND OF THE MONEY YOU PAID FOR THE SOFTWARE (LESS SHIPPING, HANDLING, AND ANY APPLICABLE TAXES EXCEPT IN CERTAIN STATES AND COUNTRIES WHERE SHIPPING, HANDLING, AND TAXES ARE REFUNDABLE) AT ANY TIME DURING THE SIXTY (60) DAY PERIOD FOLLOWING THE DATE OF PURCHASE.

1. License:

The software and documentation that accompanies this license (collectively the "Software") is the property of Symantec, or its licensors, and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that Symantec may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows.

You may:

A. use one copy of the Software on a single computer. If a License Module accompanies, precedes, or follows this license, You may make the number of copies of the Software licensed to You by Symantec as provided in Your License Module. Your License Module shall constitute proof of Your right to make such copies;

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;

D. after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and

E. use the Software in accordance with any additional permitted uses set forth below.

You may not:

A. copy the printed documentation that accompanies the Software;

B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;

D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

E. use a later version of the Software than is provided herewith unless You have purchased upgrade insurance or have otherwise separately acquired the right to use such later version;

F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

G. use the Software in any manner not authorized by this license; nor

H. use the Software in any manner that contradicts any additional restrictions set forth below.

2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content

Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

3. Product Installation and Required Activation:

There are technological measures in this Software that are designed to prevent unlicensed or illegal use of the Software. You agree that Symantec may use these measures to protect Symantec against software piracy. This Software may contain enforcement technology that limits the ability to install and uninstall the Software on a computer to not more than a finite number of times for a finite number of computers. This License and the Software containing enforcement technology require activation as further set forth in the documentation. The Software will only operate for a finite period of time prior to Software activation by You. During activation, You will provide Your unique product key accompanying the Software and computer configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If You do not complete the activation within the finite period of time set forth in the documentation, or as prompted by the Software, the Software will cease to function until activation is complete, which will restore Software functionality. In the event that You are not able to activate the Software over the Internet, or through any other method specified during the activation process, You may contact Symantec Customer Support using the information provided by Symantec during activation, or as may be set forth in the documentation.

4. Sixty (60) Day Money Back Guarantee:

If You are the original licensee of this copy of the Software and are not completely satisfied with it for any reason, please contact Symantec Customer Service for a refund of the money You paid for the Software (less shipping, handling, and any applicable taxes except in certain states and countries where shipping, handling and taxes are refundable) at any time during the sixty (60) day period following the date of purchase.

5. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

6. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software.

7. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are “Commercial Items,” as that term is defined in 48 C.F.R. section 2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States

Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

8. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. You agree to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. You agree not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, You agree not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will You sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

9. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Consumer Support, PO Box 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

10. Additional Uses and Restrictions:

A. In the event this Software contains the Norton Security Center component, any disclaimer of damages herein shall apply to such component.